Advantages Of EHRs In Health Care

Posted on March 22, 2019

Abstract

Healthcare organizations can take advantage of the use of the latest technology such as the use of EHRs that allow them to keep the record of patients' histories in electronic forms. However, there are questions regarding the use of this technology concerning privacy and security perspectives of the patient's sensitive medical data. To make this data protected and reliable, it is required to recognize the limits of the system and devise plans to protect the system. Among the most effective strategies are the use of firewalls as well as cryptography methodologies. There will also be an implementation plan discussed in the paper to make the system more effective.

Introduction

The use of technology is increasing in the healthcare sector, making the industry evolve. With the use of technology, healthcare professionals are getting more and more tools that assist them in providing quality patient care. In the past, doctors used to fill out the form and save them in the form of a patient's medical file. Then, doctors moved towards the use of computers to update medical files. One example of this is the use of Electronic Health Records (EHRs) in the health industry in recent years. More and more information in the healthcare industry is being moved to electronic form. Center for Medicare and Medicaid Services (CMS) defines EHRs as electronic health records of patient's medical history that are maintained by healthcare organizations over time (Kruse, Smith, Vanderlinden, & Nealand, 2017). EHRs are becoming common as they increase clinician efficiency due to their numerous inbuilt properties. There is a digital medical record of all the entered data along with the facility of having prescriptions by the selection of medicines from a drop-down list (Bajwa, 2014). Patients also have the facility of accessing their portal and viewing their medical records. Moreover, by using EHRs clinicians get assistance in connecting patients and managing them effectively by also connecting with fellow doctors around the world. Clinicians also take a precise sight into patients' health. On the other hand, these also assist patients in having a proper history of their illness. However, there is a drawback with these EHRs: it is becoming difficult to keep these records safe. EHRs consist of data related to patients' personal information as well as their medical histories. They are susceptible to cyber-attacks and require proper security due to the involvement of sensitive information. With these attacks, confidential health records get compromised as a result of an invasion of privacy. In this way, private medical conditions go public. To boost patients' confidence, it is needed to keep these records secure.

Patients' present and future health care largely depend on their health records. These records are

also used in the management and forecasting of healthcare facilities and services. Healthcare records are required for conducting medical research and the generation of healthcare statistics. Whenever a patient returns to the medical facility, his medical record assists healthcare providers in recovering his history and coordinating the current assessment. If there is any damage to the health record, then healthcare services that are supposed to be provided to patients effectively get affected (Weerasinghe et al., 2008). There is a recording of facts related to a patient's health in a health record to get assistance in health care services. The healthcare record consists of information related to the patient and services that were provided to him during his last visit to the healthcare center. There is also information regarding the outcome of care as well as treatment. Four main sections of the medical record contain four types of data: administrative, legal, financial as well and clinical data. Administrative data includes data related to demographic and socioeconomic characteristics of patients (sex, date, place of birth, address, medical record number). The legal data consists of the patient's consent for treatment by a specific doctor, and financial data includes the details of the patient's expenses for having the medical services. Thus, legal compliance consists of strategies to fulfill security requirements.

There are security and privacy concerns in maintaining the health records of patients as well as healthcare providers. There is a digital power that rests with internet hackers and can be used for privacy invasion. Moreover, there is a potential for misplacement of data all over this process. There are transitional strategies that eliminate data misplacement. The downsides of EHRs are because of the deficiency of technical support for maintaining security. Due to less ineffective security, it is possible for attackers to make use of data mining methods and procedures to have access to sensitive data. These then release the data to the public in the context of a data breach. These incidents are not frequent, but still, these concerns are valid. Healthcare organizations are trying to provide top-quality security to protect their software to reap the promise of digital health information. Organizations can enjoy the advantages of an electronic health system only if it is secured and saved to be used. If patients feel that the confidentiality and accuracy of their electronic health information are in danger, then they show resistance to the adoption of this system (Harman, Flite & Bond,2012. The consequences of this withholding information can be severing. Also, if there are breaches of health information, then it also impacts the organization's reputation along with damaging the patient's health and status and providing them emotional harm. Thus, it is essential to make health information secure. When there is a personal data breach, then the result is an accidental or unlawful demolition of data along with the unauthorized disclosure of data that will lead to personal data transmission. Therefore, healthcare organizations and patients will also suffer from financial losses if there are breaches of contracts as a result of privacy invasion and there is a disclosure of their billing data and PHI. Any data breach must be notified to the supervisory authority within 72 hours to protect the further damage.

There is a great difference in the security and privacy of healthcare data. Privacy is related to the capability of protecting sensitive healthcare information. The focus remains on the use and control of individuals' private data. In the case of security, the focus remains on the protection of the system against any unauthorized access. The data is protected from any malicious attack as well as from

stealing to earn a profit. In short, security is linked with confidentiality, integrity, and availability of data, while privacy is associated with the suitable user's information. Security and privacy in maintaining health records can be ensured by enhancing administrative controls. It is required by the organization to update its policies and procedures. There must be a strict privacy and security training procedure before the use of any software to maintain the health record. There must be the monitoring of physical and system access on a frequent basis with running background controls on all employees. This paper will discuss the importance of secure health records and how these can be made secure with the latest technology.

Literature Review

Electronic Health Records (EHRs) are the electronic form of a patient's health record that is factually shaped, employed and stored by healthcare organizations to assist in providing health facilities (Seymour, Frantsvog & Graeber, 2012). These records have been around since the beginning of healthcare. These records were initially used to store information related to diseases and their causes (Seymour et al., 2012). To maintain the quality of the healthcare sector, the focus then shifted towards maintaining these records electronically. EHRs have been adopted slowly, as the results of a survey showed that during 2007–2008, only 17% of clinicians adopted the system (Evans & Stemple, 2008). Thus, the use of these records was a slow process, and physicians and healthcare providers, due to the security risks associated with these records, slowly adopted the system. Among the reasons, the main reason was the heavy costs associated with the adoption of this system along with the security concerns. American Recovery and Investment Act was passed by Congress in 2009 according to which it was required by the US government to propose inducements to all healthcare suppliers for the implementation of Electronic Health Records (EHRs) (Seymour et al., 2012). Thus in compliance with this act, hospitals and physicians will be able to claim incentive payments concerning Medicare and Medicaid.

The healthcare industry is facing the issue of security and privacy as the main concern concerning the adoption of Electronic health records (EHRs), and issues have long been debated(Papoutsi et al., 2015). These issues also serve as barriers to the adoption of electronic health records. Numerous strategies have been used to address these issues. There must be the fulfillment of security and privacy requirements of the information system as the main strategy for dealing with all privacy issues. Information security is the safety of information and information systems from unlawful access, usage, exposé, interruption, alteration, or annihilation. Information security is attained by safeguarding the confidentiality, integrity, and availability of healthcare information. Confidentiality, integrity, along availability are required to be a part of the privacy attributes of any information system, and the same is the case with EHRs.

In the United States, there are also threats to healthcare data that have computerized longitudinal databases. These threats are due to technological challenges in the healthcare domain. These databases are designed to share information with patients along with doctors and researchers

(Roman, 2009). EHRs are shared among diverse arrangements, and this directness educates substantial apprehension about patient privacy because of the opportunity of unauthorized admittance. In the United States, along with other countries, this data is increasingly viewed as of great value by big data brokers (Vithiatharan, 2014). These cybercriminals find the opportunity to earn a profit with this data, and thus, this data is susceptible. Due to these reasons, comprehensive data protection systems are still in danger of being damaged by these cyber criminals. Due to this improper security implementation, this information can be misused anywhere and at any time. To secure the system, it is required to have access to only authorized users of the system. Due to privacy and security issues, patients are now unwilling to stake their health information except for direct clinical care (Rezaeibagha, Win & Susilo, 2015).

The primary purpose of the documentation is to get support in patient care, and for this purpose, there is the scanning of clinical documentation into an electronic system instantaneously which is also done at the time of patient discharge from the hospital. To protect the whole procedure, the government also enforced certain acts to protect the sensitive information of users. Patient electronic health records have added confidentiality and security of protected health information (PHI) as a requirement of the Health Insurance Portability and Accountability Act (HIPAA). Congress passed this act in 1996, but till 2005, it was not required under this act to comply with this act's sub-rulings. Under HIPAA, organizations are needed to carry out audit trails along with the documentation of information systems activity. With the audit trials, they get enabled to qualify for incentive payments from Medicare and Medicaid. HIPAA has outlined three pillars for safeguarding protected health information, and these include administrative safeguards, physical safeguards as well as technical safeguards. These safeguards range from a site of computers to the practice of firewall software to guard health information(Kruse et al., 2017). Administrative safeguards consist of audits, an appointment of a chief information security officer, as well as scheming of different contingency plans. Moreover, physical safeguards include assigning security accountabilities, workplace safety as well as physical access controls. The third category, technical safeguards, is linked to the protection of data and information systems that exist in health organizations. After HIPPA, there came another act in 2003 by the US government, known as the Health Information Technology for Economic and Clinical Health (HITECH) Act. The strategies defined in this act ensure the privacy and security of patient information and also inform patients whenever their privacy is compromised. This act is related to the breach of personal health information that can happen as a result of interference from both internal and external sources.

Many techniques can be used for securing health records, and these include cloud computing, firewalls, antivirus software, cryptography, and chief information security officers (CISOs) (Kruse et al., 2017). Among these techniques, the most common is the use of firewalls to protect healthcare organizations' information technology systems. While going for firewalls, there is a need to apply all four points of the firewall security strategies. These include service control, direction control, user control as well as behavior control. However, before applying any firewall, it is required by an organization needs to have a complete needs assessment of the healthcare organization along with a complete threat assessment. These must be performed both internally and externally. If these

assessments are not completed before the application of any firewall, then the security of patients will be at stake all the time.

However, this is a rather costly technique, and expenses depend on the size and scope of an organization. But at the same time, it is also a successful technique that secures the healthcare information of an organization. An organization can be protected both internally and externally with the use of different kinds of firewalls. There can be the use of a packet filtering firewall that is aimed to filter internal electronic feeds as well as stop the outside feeds from entering the organization's network. This is the same as any organization putting restrictions over a certain internet protocol (IP) address to enter the system. With packet filtering farewell, another kind is status inspection firewalls, which are much more dynamic. This farewell cannot only find the association with the incoming electronic feeds, but it can also verify the incoming electronic feeds. Application level gateway, a category of farewell, can also be used for security and maintaining privacy. Thus, firewalls establish a secure communication channel.

Cryptography as a technique can be used to ensure the safety of health information in electronic health records systems. During the exchange of health information, encryption specifically serves the purpose, and this is according to the Health Insurance Portability and Accountability Act (HIPAA). For example, there can be the use of digital signatures that can stop the breach of PHI while dealing with patients' personal information. This method is also effective in the case of the use of mobile agents for transmitting patients among different facilities. Cryptography usage in a system also allows the practice of usernames and passwords.

In addition to this, there is an important role of consent in maintaining patients' privacy. Informed consent in health care refers to the patient's awareness regarding his medical status and his approval for the sharing of information. This information is released to others with the patient's consent as specified by law. This does not imply that physicians have no access to patient information. Information can be used with patient consent and patients have federal, state, and legal rights in this regard so that their privacy must not be compromised in this system. Therefore, patients must have control over their data so that they can decide regarding access to their sensitive health data (Marinič, 2015). Written patient consent is necessary for the form of a data protection agreement in this context. Thus, hospitals must be made responsible for notifying patients regarding the usage of their data and obtaining consent before revealing their data. Consequently, US law protects this data that circulates within its health care system.

The United States government has also passed legislation that requires healthcare providers to adopt this system and maintain Electronic Health Records by 2015, as healthcare providers were adopting them slowly. For example, the federal health data protection model is required to show the inclusive charting of the healthcare industry. There are also monetary penalties for not using electronic records in any healthcare organization.

Problems & Recommendation

A medical record is a communication tool, either paper-based or electronic, that is used to assist in clinical decision-making. This record is also used for providing assistance in coordinating the services and in the form of business records. The essential feature of this record is that it must be authenticated to serve the purpose. Today, healthcare organizations are using this record in the form of Electronic Health Records (EHRs). EHRs can record medical and treatment accounts of the patient, details about diagnoses, medicines, and immunization times, in addition to details of different laboratory tests. Physicians, just with the touch of a button or click of a mouse, can view these details as in this system, lab results also spontaneously are connected to the patient's health record when these get uploaded to the diagnostic lab's Server (Bajwa, 2014). There is also the facility of prescriptions available in these records, and these are automatically transmitted to the patients' pharmacies. These electronic health records have the potential to assimilate statistics from multiple sources and deliver a more inclusive interpretation of patient care. These are also aimed at delivering admission to implements as clinical decision support. They are enjoying many benefits of this system as the availability of information securely to be used by several sanctioned users. These are thus viewed by numerous users at the same time with the use of information technology tools. One of the users of these records is patients that routinely assess their electronic health records and maintain personal health records (PHR), comprising of clinical documentation related to their diagnoses. PHRs provide opportunities for disabled people to have a user-friendly interface (Kaelber et al., 2008). For instance, they can increase the font size and translate text to sound for a proper understanding of their health information.

Thus, the challenges that the U.S. healthcare system aspects on numerous heads, counting mounting costs along with unreliable quality, are addressed to a great extent with the use of EHRs. Despite having all these advantages, these are still not safe to use in healthcare organizations, and both patients as well as healthcare organizations show their apprehension towards the security of the system. This record is the patient information, but it is owned by the healthcare organization, and its security is the responsibility of the healthcare organization. Therefore, there are three main ethical significances for these electronic health records; privacy and confidentiality, security as well as data integrity, and availability. Confidentiality here is linked with a physician-patient relationship; any information related to this relationship must not be revealed without patient consent (Lafky & Horan, 2011). The integrity of personal information is also important as if there is any change in data or there is inaccuracy present in the data then it will negatively impact the healthcare process. There must be integrity in EHRs so that health care professionals can avail of the information readily at the time when it is required. Similarly, the security of EHR is linked with the physical security of information. When there is an advancement in technology, then access to information increases. But for protection, this access must be limited.

Organizations must review their health information security policies and cultivate new policy declarations to address the new risks associated with electronic health information. New policy

declarations may incorporate the use of certain technologies, such as encryption of data on laptops. There can also be strategies related to access to this information by patients. Numerous strategies can be devised for making the EHRs secure. These strategies can be administrative as well as technical. There are rules and regulations set by HIPAA that need to be followed by organizations to protect patient data from unauthorized access. According to HIPAA, a user of EHRs must not leave any printed patient health information open, as it can be accessed by anyone when it has physical availability. Thus, the paper copy must be destroyed after scanning information into a patient's EHR(Kruse et al., 2017). Computer screens are easy to view as compared to a paper copy. Thus, it is required to set paper screens in such a way as to minimize their visibility by outsiders to the system. In order not to have a side view of the system, it is also required to use privacy filters on monitors. The use of antivirus and intrusion detection and firewall software must be a part of security checks in healthcare organizations. Moreover, patients must not be identified with any social security number. Patient authorization is needed for the purpose of sharing information. This information in EHRs must be protected from marketers along with employers and immigration officers.

Care must also be taken while accessing the information from outside of the office. Use only a secure Internet connection for doing this, and also do not open the information in such a way that it becomes visible to people. It is required by every healthcare organization to form policies and procedures related to data security and train its employees for the use and enforcement of these policies and procedures. These must be understood by every user of the system to ensure the security of the system. According to HIPAA requirements, staffing changes must be updated timely, and the user status of the former employee must be changed to inactive. In this way, they will not be able to log in using their old password, and the system will be protected from any unauthorized access. After using the system, users must log out to protect the system from outside access. If there is no proper logout, then the patient data screen will be opened, and unauthorized users will be able to acquire the information from the system. In any case, there must be confidentiality of information that includes the name of the patient and address along with his social security number and date of birth. Along with this personal information included in the list is also the information related to his emotional and financial conditions.

In addition to the security and privacy issues, there are some drawbacks of the system that need to be addressed. There is an immense cost associated with the use and adoption of the system. Thus, small hospitals should align themselves with larger hospitals to effectively distribute the high costs of the system, as small organizations have limited resources (Seymour et al., 2012). It will take almost three years to cover the costs and then there will be profits from the adoption of this system both in financial and non-financial terms. Also, due to EHR, there is an increased documentation time. This must be synchronized with the daily operations in such a way that clinicians do not consider it a burden to be implemented forcefully. Systems sometimes get slow, either due to software or hardware. Moreover, there is a requirement for data integrity as an essential feature of EHRs. There must not be the feature of copying and paste of content available in the system without any justification, as then the integrity of the system is compromised. This shortcut of copy and paste is to reduce the amount of time consumed by monitors. But at the same time, it is also a potential source

of threat to patient safety. Thus, there must be such EHR designs implemented that can increase the prominence of information being designated for copy and paste to stop the users from unintentionally copying unwanted parts of information.

Another strategy in this regard can be to lock certain areas of information so that there cannot be any copy-and-paste option enabled for the users as copy and paste function can be disabled in EHRs when there is data entering. This will reduce the risks of misuse of information as well as mistakes in documentation which mostly happen while entering data in blood transfusions. Moreover, the possibly tricky feature is the drop-down menu that can limit the available choices for a diagnosis. Clinicians only make selections from the drop-down menu, which can cause errors. Clinicians, along with vendors, have been employed to solve the software problems that include the screen design along with drop-down menus.

From this discussion, it can be concluded that EHRs are best when they are simple as these increase usability. Simple EHRs allow users to get information in a clear, concise, and straightforward way and fewer errors. This reduces the risk of patient safety problems. But, if these are complex, they create confusion for the users and negatively affect clinical output. Similarly, if these are poorly designed then these also become a source of confusion for the users. There must also be enhanced communication between health IT developers and providers. This measure will help in avoiding costly, long-term software problems associated with EHR technology.

EHR technology is in danger of cyber-attacks due to the use of the Internet of Medical Things (IoT). These devices do not have security as a primary concern. Thus, these are the striking entryway into healthcare systems for cybercriminals. Manufacturers of these devices are also not restricted by HIPAA regulations that need security structures to guard the PHI of patients. Along with the lacking of initial infrastructural security features, these are also not associated with any security-connected updates and coverings whenever there is a new susceptibility discovered. These devices are also programmed for the patients to have access to their records. Thus, these are structured in such a way as to provide a maximum number of endpoints along with applications for the ease of patients. There is a need to make these endpoints secure for the safety of the whole system. All the structures of the system must be designed in such a way that will increase the safety of the system from any cyber-attack. Patients make use of email and texting to communicate electronically with their providers. For security, while sending ePHI to a patient, there is a need to send it via a secure method. This will make sure that it will be delivered to the intended recipient. However, this rule is not applicable to a patient, and he is allowed to send health information via email or texting. HIPAA Rules are always there to protect and receive information and encrypt messages that can be used when there is more communication using the email system. Also, Heath care organizations, which are using the EHR technology, must appoint a data protection officer. He will be responsible for ensuring all the measures related to security and making the system more and more secure from any external attack.

Implementation Plan

After completing the risk assessments under HIPAA rules, there will be implementation strategies for compliance with HIPAA rules. Strategies will be made to address the issues in safeguarding the physical, technical, and administrative dimensions concerning security and privacy matters. Firstly, there will be the dissemination of privacy and security policies among healthcare organizations' staff. This will make sure that all policies are properly communicated will all staff members to get compliance from all the staff prompt manner and leave no loophole for any security concern. The implementation plan will ensure that not all policies are just communicated, but they are also fully understood by all the staff members. With the staff members, there will also be a discussion regarding the organization's expectations and objectives regarding the use of EHRs, as, ultimately, these are people who are responsible for the proper implementation of all the strategies and responsible for the security of all health-related information.

Save all the steps of this implementation plan in an electronic folder to address the need for the revival of any strategy at any time to achieve the objectives. For example, there will be a record of all the checklists along with the security risk analysis in files. Staff training records will be updated promptly to be assessed at the end of the plan to judge the correct course of implementation. It is necessary to have a record of all these steps for audit.

Concerning administrative safeguards, there will be continual risk assessment of the health IT environment. This assessment will include the effectiveness of safeguards for electronic health information. Firstly, a system should be password protected besides encrypted and proper log out must also be ensured along with this password usage. Thus, system data will be shared using the proper password, and these must also be encrypted to ensure further safety. The access to data must also be limited to the staff and another person will be allowed to view the sensitive information for any purpose. There is a dashboard in the system that is provided with administrative access options. Thus, it is not difficult to apply all these changes and strategies. Also, every healthcare organization must ensure that patient information is only accessed when there is a need to know the information, and it must be discarded appropriately after use. In this respect, there can be the use of locked trash bins or the use of shredders. To access the information, there must be forwarded requests for patients' medical records (Ozair et al., 2015). Patient charts or files must also not be left unattended to ensure the safety of information. Patient confidentiality is the responsibility of every individual in the healthcare organization: board members, executive leadership, clinical staff, physicians, nurses, administrative and clerical staff, as well as students and interns.

For this purpose, there will be an arrangement of employee training so that they may be able to use health IT appropriately with the purpose of protecting electronic health information. If employees are not using the system effectively, they will not enter data correctly thus causing inaccurate diagnoses and inaccurate treatments. Patient data is also not saved if there is a lack of training, leading to increased security concerns. There will also be a mechanism to report security breaches so that the

continuity of health operations can be ensured. If there is a data breach in which at least 500 people's information is being compromised, then this data breach must be reported with specific details by the healthcare organization as required by the HITECH Act (Kruse et al., 2017). Thus, the main aim of the HITECH Act is to nurture significant usage of certified EHR expertise. Under the HITECH Act, ONC is the main organization in the federal government that is responsible for evolving and synchronizing nationally HIT policy and endorsing the growth of a national health IT organization for the usage and interchange of electronic health evidence.

Moreover, included in the implementation plan will be physical safeguards. There will be the arrangement of office alarms on the premises that will make use of EHRs. Computing equipment will also be locked physically to safeguard them from any physical damage. Technical safeguards will include virus checking, along with the use of different firewalls. There will also be the use of cloud service providers (CSPs) to add-on HIT infrastructure growth (Page et al., 2015). This will not only assist in data storage and recover their cybersecurity degree, but will also make the system up to date according to the latest technology.

To reduce the associated costs, there will be a need to maintain fewer PHRs. Multiple providers in dissimilar organizations are checking some patients, and the result is the maintenance of multiple PHRs. It costs more when there is data retrieval from multiple PHRs along with the issue of quality. The solution to this is the maintenance of only one PHR by the patient. Thus, patients must also be encouraged to have only one PHR so that their information remains safe, and they must be relieved from the burden of healthcare costs.

Above all, there will be the arrangement of sufficient funding to have the increased use of EHRs across the organization as organizations due to heavy costs, face difficulty in applying the use of this system all over the healthcare organization. There will be the use of grants and loans for arranging the funds to have a successful implementation plan for amending the security issues in EHRs. The funding will also be needed to make the technology used in EHRs updated as technology is evolving every day, and it requires investment to make it the latest technology to be used in healthcare organizations.

Conclusion

EHRs are the electronic version of the paper-based health records of patients consisting of their medical histories. Included in these medical histories are information related to disease symptoms, and diagnoses along with the information related to lab results and the summary of the details of immunizations. EHRs are designed according to the organization's requirements, and these vary regarding contents as well as functionality. With the use of these records, healthcare organizations are providing competent and real-time services to patients (Roman, 2009). These records allow doctors to recover the health conditions of patients suffering from different ailments and save lives. Doctors are now making more and more use of these technologies to gather information and use this

in improving patients' health conditions. These records are related to patients' personal health information, and thus, patients have privacy rights for these records.

Privacy and security concerns are serving as the largest blockade to electronic health record acceptance. Consequently, it is imperious for health organizations to classify techniques to save electronic health records from any cyber activity along with the physical threat to the information (Kruse et al., 2017). One strategy in this regard can be that only authorized users can make use of these records, as information in these records is only shared with these users with patient consent. However, due to the digital nature of electronic healthcare systems, unauthorized users can also access these records. These users target patient data to earn a profit. To prevent this interference, numerous security techniques are associated with the size and scope of a healthcare organization. When information is made secure, then trust is built between patients along providers.

An internet connection is inevitable for carrying out online activities as a part of the EHR setup. All the activities are in EHRs; the exchange of patient information, submission of claims as well as generation of electronic records are included in online activities. There is a need for such a cyber-security that will address these issues. Among the numerous techniques, firewalls and cryptography are successfully used in healthcare organizations. These will protect the stored digital assets and make the system free from any cyber-attack. These are applicable in both situations; when these are installed locally as well as when these are accessed over the Internet using a cloud service provider.

Thus, to improve communication and efficiency, there is a need to use the latest technology in the healthcare sector, such as EHRs. However, with the use of EHRs, there is an increased risk of cyber-attacks due to the presence of IoMT devices. This must be addressed with the proper measures to make this technology more effective. There is a bright future concerning EHR technology, and there are many strategies that can be adapted to make this technology more and more secure. This technology is enabling us to adjust to the high costs of the medial related issues in the US, and these are providing new opportunities such as data mining. With healthcare data mining, it is possible to predict potential patients with potential diseases. This data can also be used by the federal government to collect data and make new healthcare plans, along with the use of this by researchers in the medical field. Thus, with the wide applications of EHRs becoming widely used, it will be possible to share healthcare data along the healthcare continuum. EHR-related safety apprehensions might not always be noticeable to users, or users can be ignorant of the cause of the troubles. For this reason, there must be a successful implementation plan on a timely basis to avoid any issue related to the privacy and security of health-related information.

References

Bajwa, M. (2014). Emerging 21st century medical technologies. *Pakistan journal of medical sciences*, *30*(3), 649.

Evans, S., & Stemple, C. (2008). Electronic health records and the value of health IT. *J Manag Care*

Pharm, *14*(6), 16-18.

Harman, L. B., Flite, C. A., & Bond, K. (2012). Electronic health records: privacy, confidentiality, and security. *Virtual Mentor*, *14*(9), 712.

Kaelber, D. C., Jha, A. K., Johnston, D., Middleton, B., & Bates, D. W. (2008). A research agenda for personal health records (PHRs). *Journal of the American Medical Informatics Association*, *15*(6), 729-736.

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security Techniques for the Electronic Health Records. *Journal of Medical Systems*, *41*(8), 127.

Lafky, D. B., & Horan, T. A. (2011). Personal health records: Consumer attitudes toward privacy and security of their personal health information. *Health Informatics Journal*, *17*(1), 63-71.

Marinič, M. (2015). The importance of health records. *Health*, *7*(05), 617.

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: a general overview. *Perspectives in clinical research*, *6*(2), 73.

Papoutsi, C., Reed, J. E., Marston, C., Lewis, R., Majeed, A., & Bell, D. (2015). Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. *BMC medical informatics and decision making*, *15*(1), 86.

Page, A., Kocabas, O., Soyata, T., Aktas, M., & Couderc, J. P. (2015). Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance. *Annals of Noninvasive Electrocardiology*, *20*(4), 328-337.

Roman, L. (2009). Combined EMR, EHR and PHR manage data for better health. *Drug Store News*, *31*(9), p40-78.

Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: technical perspectives. *Health Information Management Journal*, *44*(3), 23-38.

Seymour, T., Frantsvog, D., & Graeber, T. (2012). Electronic health records (EHR). *American Journal of Health Sciences*, *3*(3), 201.

Vithiatharan, R. N. (2014). The potentials and challenges of big data in public health.

Weerasinghe, D., Rajarajan, M., Elmufti, K., & Rakocevic, V. (2008). Patient privacy protection using anonymous access control techniques. *Methods of Information in Medicine*, *47*(03), 235-240.